INTERNATIONAL SEARCH REPORT

International application No.
PCT/US00/02170

A. CLASSIFICATION OF SUBJECT MATTER

IPC(7) :H04L 9/00, 08, 14, 16
US CL : 380/281, 282, 284, 285, 45

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

U.S. : 380/281, 282, 284, 285, 45

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No
Y	US 5,503,287 A (MORRIS et al) 05 MARCH 1985, abstract, figure 3, summary	1-15
Y	US 5,144,665 A (TAKARAGI et al) 01 SEPTEMBER 1992, abstract, figure 2, summary	1-15
Y	MENEZES et al. HANDBOOK OF APPLIED CRYPTOGRAPHY, 17 OCTOBER 1996, pp. 551-553	1-15
A	US 5,237,611 A (RASMUSSEN et al) 17 AUGUST 1993, abstract	1-15

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

*	Special categories of cited documents	"T"	later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A"	document defining the general state of the art which is not considered to be of particular relevance	"X"	document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"E"	earlier document published on or after the international filing date	"Y"	document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"L"	document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"&"	document member of the same patent family
"O"	document referring to an oral disclosure, use, exhibition or other means		
"P"	document published prior to the international filing date but later than the priority date claimed		

Date of the actual completion of the international search	Date of mailing of the international search report
21 APRIL 2000	

Name and mailing address of the ISA/US	Authorized officer
Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231	GAIL HAYES James R. Matthews
Facsimile No. (703) 305-3230	Telephone No. (703) 308-3900

PATENT COOPERATION TREATY

From the
INTERNATIONAL PRELIMINARY EXAMINING AUTHORITY

To: CHARLES J. KULAS
TOWNSEND AND TOWNSEND AND CREW LLP
TWO EMBARCADERO CENTER
8TH FLOOR
SAN FRANSISCO, CA 94111-3834

PCT

WRITTEN OPINION

(PCT Rule 66)

Date of Mailing *(day/month/year)*	29 DEC 2000
Applicant's or agent's file reference 18926-410PC	REPLY DUE within TWO months from the above date of mailing

International application No.	International filing date *(day/month/year)*	Priority date *(day/month/year)*
PCT/US00/02170	28 JANUARY 2000	29 JANUARY 1999

International Patent Classification (IPC) or both national classification and IPC
IPC(7): H04L 9/00, 9/08, 9/14,9/16 and US Cl.:380/281, 282, 284, 285, 45

Applicant
GENERAL INSTRUMENT CORPORATION

1. This written opinion is the first (first, etc.) drawn by this International Preliminary Examining Authority.

2. This opinion contains indications relating to the following items:

- I [X] Basis of the opinion
- II [ ] Priority
- III [ ] Non-establishment of opinion with regard to novelty, inventive step or industrial applicability
- IV [ ] Lack of unity of invention
- V [X] Reasoned statement under Rule 66.2(a)(ii) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
- VI [ ] Certain documents cited
- VII [ ] Certain defects in the international application
- VIII [ ] Certain observations on the international application

3. The applicant is hereby invited to reply to this opinion.

When? See the time limit indicated above. ~~The applicant may, before the expiration of that time limit, request this Authority to grant an extension., see Rule 66.2(d).~~

How? By submitting a written reply, accompanied, where appropriate, by amendments, according to Rule 66.3. For the form and the language of the amendments, see Rules 66.8 and 66.9.

Also For an additional opportunity to submit amendments, see Rule 66.4.
For the examiner's obligation to consider amendments and/or arguments, see Rule 66.4 *bis*.
For an informal communication with the examiner, see Rule 66.6.

If no reply is filed, the international preliminary examination report will be established on the basis of this opinion.

4. The final date by which the international preliminary examination report must be established according to Rule 69.2 is: 29 MAY 2001

Name and mailing address of the IPEA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703) 305-3230	Authorized officer Peggy Harwood GAIL HAYES Telephone No. (703) 306-5975

Form PCT/IPEA/408 (cover sheet) (July 1998)*

WRITTEN OPINION

International application No.
PCT/US00/02170

I. Basis of the opinion

1. With regard to the **elements** of the international application:*

[X] the international application as originally filed

[X] the description:
pages 1-13 , as originally filed
pages NONE , filed with the demand
pages NONE , filed with the letter of

[X] the claims:
pages 14-16 , as originally filed
pages NONE , as amended (together with any statement) under Article 19
pages NONE , filed with the demand
pages NONE , filed with the letter of

[X] the drawings:
pages 1-3 , as originally filed
pages NONE , filed with the demand
pages NONE , filed with the letter of

[X] the sequence listing part of the description:
pages NONE , as originally filed
pages NONE , filed with the demand
pages NONE , filed with the letter of

2. With regard to the **language**, all the elements marked above were available or furnished to this Authority in the language in which the international application was filed, unless otherwise indicated under this item.
These elements were available or furnished to this Authority in the following language _____ which is:

[ ] the language of a translation furnished for the purposes of international search (under Rule 23.1(b)).

[ ] the language of publication of the international application (under Rule 48.3(b)).

[ ] the language of the translation furnished for the purposes of international preliminary examination (under Rules 55.2 and/or 55.3).

3. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, the written opinion was drawn on the basis of the sequence listing:

[ ] contained in the international application in printed form.

[ ] filed together with the international application in computer readable form.

[ ] furnished subsequently to this Authority in written form.

[ ] furnished subsequently to this Authority in computer readable form.

[ ] The statement that the subsequently furnished written sequence listing does not go beyond the disclosure in the international application as filed has been furnished.

[ ] The statement that the information recorded in computer readable form is identical to the writen sequence listing has been furnished.

4. [X] The amendments have resulted in the cancellation of:

[X] the description, pages NONE

[X] the claims, Nos. NONE

[X] the drawings, sheets/~~fig~~ NONE

5. [ ] This opinion has been drawn as if (some of) the amendments had not been made, since they have been considered to go beyond the disclosure as filed, as indicated in the Supplemental Box (Rule 70.2(c)).

** Replacement sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this opinion as "originally filed".*

WRITTEN OPINION

International application No.
PCT/US00/02170

V. Reasoned statement under Rule 66.2(a)(ii) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. statement

Novelty (N)	Claims	1-15	YES
	Claims	NONE	NO
Inventive Step (IS)	Claims	NONE	YES
	Claims	1-15	NO
Industrial Applicability (IA)	Claims	1-15	YES
	Claims	NONE	NO

2. citations and explanations

Claims lack 1-15 an inventive step under PCT Article 33(3) as being obvious over Menezes et al in view of Schneier.

Claim 1 is directed to a two-level asymmetric cryptosystem. Menezes et al disclose the technique of key layering in which a key encrypting key protects a second key, see section 13.3.1. Menezes et al disclose that the keys may be asymmetric, see figure 13.4. Menezes et al disclose that the key encrypting key is a long term key and the protected key is a short term key. Schneier disclose that different lifetimes of keys correspond to different key usages such as key encrypting key or protected keys, see section 8.10. Schneier also discloses that different key lifetimes correspond to different key lengths and therefore to different processing operations and rates. It would therefore be obvious to construct a two level asymmetric cryptographic processing system where a first key protects a second key with the first key having a longer lifetime, keylength, and processing rate.

Claims 2-5 are directed to sending various types of data over computer networks. All of these types of data are well-known to be subjected to encryption and transmission over networks. Each of these claims are obvious uses for the system of claim 1.

Claim 6 differs from claim 2 in that the key is hard coded into the system. Hard coding keys in systems for sending voice data over networks is an obvious expedient for having the transmitter access the encryption keys used to encrypt data.

Claim 7 differs from claim 6 in that the communications system is part of a network containg like systems. This is an obvious usage for cryptographic devices used to send data over a network, such as a pair of encrypted telephones. The limitations of claim 7 are well known over the disclosures of Menezes et al and Schneier.

Claim 8 is a method claim embodiment of claim 1 and is obvious for analogous and additionally the following grounds. The main difference between the inventions of claims 1 and 8 is that a key (Continued on Supplemental Sheet.)

PATENT COOPERATION TREATY

From the
INTERNATIONAL PRELIMINARY EXAMINING AUTHORITY

To: CHARLES J. KULAS
TOWNSEND AND TOWNSEND AND CREW LLP
TWO EMBARCADERO CENTER
8TH FLOOR
SAN FRANCISCO, CA 94111-3834

PCT

NOTIFICATION OF TRANSMITTAL OF INTERNATIONAL PRELIMINARY EXAMINATION REPORT

(PCT Rule 71.1)

Date of Mailing *(day/month/year)*	20 JUN 2001
Applicant's or agent's file reference 18926-410PC	IMPORTANT NOTIFICATION

International application No.	International filing date *(day/month/year)*	Priority Date *(day/month/year)*
PCT/US00/02170	28 JANUARY 2000	29 JANUARY 1999

Applicant
GENERAL INSTRUMENT CORPORATION

1. The applicant is hereby notified that this International Preliminary Examining Authority transmits herewith the international preliminary examination report and its annexes, if any, established on the international application.

2. A copy of the report and its annexes, if any, is being transmitted to the International Bureau for communication to all the elected Offices.

3. Where required by any of the elected Offices, the International Bureau will prepare an English translation of the report (but not of any annexes) and will transmit such translation to those Offices.

4. **REMINDER** 7/29/01

The applicant must enter the national phase before each elected Office by performing certain acts (filing translations and paying national fees) within 30 months from the priority date (or later in some Offices)(Article 39(1))(see also the reminder sent by the International Bureau with Form PCT/IB/301).

Where a translation of the international application must be furnished to an elected Office, that translation must contain a translation of any annexes to the international preliminary examination report. It is the applicant's responsibility to prepare and furnish such translation directly to each elected Office concerned.

For further details on the applicable time limits and requirements of the elected Offices, see Volume II of the PCT Applicant's Guide.

Name and mailing address of the IPEA/US	Authorized officer
Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231	GAIL HAYES Peggy Harwood
Facsimile No. (703) 305-3230	Telephone No. (703) 306-5975

Form PCT/IPEA/416 (July 1992) ★

PATENT COOPERATION TREATY

PCT

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

(PCT Article 36 and Rule 70)

Applicant's or agent's file reference 18926-410PC	**FOR FURTHER ACTION**	See Notification of Transmittal of International Preliminary Examination Report (Form PCT/IPEA/416)
International application No. PCT/US00/02170	International filing date *(day/month/year)* 28 JANUARY 2000	Priority date *(day/month/year)* 29 JANUARY 1999
International Patent Classification (IPC) or national classification and IPC IPC(7): H04L 9/00, 08, 14, 16 and US Cl.: 380/281, 282, 284, 285, 45		
Applicant GENERAL INSTRUMENT CORPORATION		

1. This international preliminary examination report has been prepared by this International Preliminary Examining Authority and is transmitted to the applicant according to Article 36.

2. This REPORT consists of a total of 4 sheets.

   ☐ This report is also accompanied by ANNEXES, i.e., sheets of the description, claims and/or drawings which have been amended and are the basis for this report and/or sheets containing rectifications made before this Authority. (see Rule 70.16 and Section 607 of the Administrative Instructions under the PCT).

   These annexes consist of a total of _____ sheets.

3. This report contains indications relating to the following items:

   - I ☒ Basis of the report
   - II ☐ Priority
   - III ☐ Non-establishment of report with regard to novelty, inventive step or industrial applicability
   - IV ☐ Lack of unity of invention
   - V ☒ Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
   - VI ☐ Certain documents cited
   - VII ☐ Certain defects in the international application
   - VIII ☐ Certain observations on the international application

Date of submission of the demand 22 AUGUST 2000	Date of completion of this report 18 MAY 2001
Name and mailing address of the IPEA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703) 305-3230	Authorized officer GAIL HAYES Telephone No. (703) 306-5975

Form PCT/IPEA/409 (cover sheet) (July 1998) ★

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No.
PCT/US00/02170

I. Basis of the report

1. With regard to the **elements** of the international application: *

[X] the international application as originally filed

[X] the description:
pages 1-13 , as originally filed
pages NONE , filed with the demand
pages NONE , filed with the letter of _____

[X] the claims:
pages 14-16 , as originally filed
pages NONE , as amended (together with any statement) under Article 19
pages NONE , filed with the demand
pages NONE , filed with the letter of _____

[X] the drawings:
pages 1-3 , as originally filed
pages NONE , filed with the demand
pages NONE , filed with the letter of _____

[X] the sequence listing part of the description:
pages NONE , as originally filed
pages NONE , filed with the demand
pages NONE , filed with the letter of _____

2. With regard to the **language**, all the elements marked above were available or furnished to this Authority in the language in which the international application was filed, unless otherwise indicated under this item.
These elements were available or furnished to this Authority in the following language _____ which is:

[ ] the language of a translation furnished for the purposes of international search (under Rule 23.1(b)).

[ ] the language of publication of the international application (under Rule 48.3(b)).

[ ] the language of the translation furnished for the purposes of international preliminary examination (under Rules 55.2 and/or 55.3).

3. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, the international preliminary examination was carried out on the basis of the sequence listing:

[ ] contained in the international application in printed form.

[ ] filed together with the international application in computer readable form.

[ ] furnished subsequently to this Authority in written form.

[ ] furnished subsequently to this Authority in computer readable form.

[ ] The statement that the subsequently furnished written sequence listing does not go beyond the disclosure in the international application as filed has been furnished.

[ ] The statement that the information recorded in computer readable form is identical to the writen sequence listing has been furnished.

4. [X] The amendments have resulted in the cancellation of:

[X] the description, pages NONE

[X] the claims, Nos. NONE

[X] the drawings, sheets/~~fig~~ NONE

5. [ ] This report has been drawn as if (some of) the amendments had not been made, since they have been considered to go beyond the disclosure as filed, as indicated in the Supplemental Box (Rule 70.2(c)).**

** Replacement sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to this report since they do not contain amendments (Rules 70.16 and 70.17).*

***Any replacement sheet containing such amendments must be referred to under item 1 and annexed to this report.*

V. Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. statement

Novelty (N)	Claims	1-15	YES
	Claims	NONE	NO
Inventive Step (IS)	Claims	NONE	YES
	Claims	1-15	NO
Industrial Applicability (IA)	Claims	1-15	YES
	Claims	NONE	NO

2. citations and explanations (Rule 70.7)

Claims lack 1-15 an inventive step under PCT Article 33(3) as being obvious over Menezes et al in view of Schneier.

Claim 1 is directed to a two-level asymmetric cryptosystem. Menezes et al disclose the technique of key layering in which a key encrypting key protects a second key, see section 13.3.1. Menezes et al disclose that the keys may be asymmetric, see figure 13.4. Menezes et al disclose that the key encrypting key is a long term key and the protected key is a short term key. Schneier disclose that different lifetimes of keys correspond to different key usages such as key encrypting key or protected keys, see section 8.10. Schneier also discloses that different key lifetimes correspond to different key lengths and therefore to different processing operations and rates. It would therefore be not require an inventive step to construct a two level asymmetric cryptographic processing system where a first key protects a second key with the first key having a longer lifetime, keylength, and processing rate.

Claims 2-5 are directed to sending various types of data over computer networks. All of these types of data are well-known to be subjected to encryption and transmission over networks. Each of these claims are obvious uses for the system of claim 1.

Claim 6 differs from claim 2 in that the key is hard coded into the system. Hard coding keys in systems for sending voice data over networks is an obvious expedient for having the transmitter access the encryption keys used to encrypt data.

Claim 7 differs from claim 6 in that the communications system is part of a network containg like systems. This is an obvious usage for cryptographic devices used to send data over a network, such as a pair of encrypted telephones. The limitations of claim 7 are well known over the disclosures of Menezes et al and Schneier.

Claim 8 is a method claim embodiment of claim 1 and is obvious for analogous and additionally the following grounds. The main difference between the inventions of claims 1 and 8 is that a key (Continued on Supplemental Sheet.)

Supplemental Box
(To be used when the space in any of the preceding boxes is not sufficient)

Continuation of: Boxes I - VIII

V. 2. REASONED STATEMENTS - CITATIONS AND EXPLANATIONS (Continued):
update is disclosed in claim 8. Schneier discloses this expedient, see section 8.10.

Claim 9 differs from claim 8 in that the method embodiment of claim 8 is embodied in a computer readable medium. That is, claim 9 is a software embodiment. Embodying computer implemented methods in software is obvious.

Claim 10 is directed to a method of providing secure data transactions over a network. Claim 10 also discloses a key update procedure using a key encrypting key. Claim 10 is obvious for reasons analogous to the reasons given above in relation to claims 1, 7, and 8. See Menezes et al, section 13.3.1 and Schneier section 7.5, and 8.10.

Claim 11 differs from claim 7 in that a third level is added to update the key encrypting key. Menezes et al disclose such a third level and employ a "master key" for such a purpose, see section 13.3.1.

Claims 12-15 specify some of the types of resources as in claim 11. Schneier discloses processing time as a type of such resource, see table 7.10. The other resources, namely transistor density, memory, and bandwidth, are obvious variation due to the well-known time-memory tradeoff in such resource intensive computer actions as cryptography or cryptanalysis.

---------- NEW CITATIONS ----------
Schneier. Applied Cryptography Second Edition. 18 October 1995. pages 165-168 and 183-184.